AMENDMENTS TO THE CLAIMS

1-22. (Cancelled)

23. (New) A method for requesting an encryption key by a subscriber station in a wireless communication system, the method comprising:

determining a service type of a traffic connection;

transmitting a first message including an identifier corresponding to the service type that requests the encryption key to a base station; and

receiving a second message from the base station.

24. (New) The method as claimed in claim 23, wherein the first message is a key request message.

25. (New) The method as claimed in claim 24, wherein the second message is a key reply message including the encryption key corresponding to the service type.

26. (New) The method as claimed in claim 23, wherein the service type is one of a unicast service, a multicast service, and a broadcast service.

27. (New) The method as claimed in claim 23, wherein when the service type is a multicast service, the first message includes an identifier of a multicast service group of a subscriber.

28. (New) A method for distributing an encryption key by a base station in a wireless communication system, the method comprising:

receiving a first message including an identifier corresponding to a service type of a traffic connection to request the encryption key from a subscriber station;

generating the encryption key corresponding to the service type; and

transmitting a second message including the encryption key to the subscriber station.

29. (New) The method as claimed in claim 28, wherein the first message is a key request message.

30. (New) The method as claimed in claim 29, wherein the second message is a key reply message including the encryption key corresponding to the service type.

31. (New) The method as claimed in claim 28, wherein the service type is one of a unicast service, a multicast service, and a broadcast service.

32. (New) The method as claimed in claim 28, wherein when the service type is a multicast service, the first message includes an identifier of a multicast service group of a subscriber.

33. (New) The method as claimed in claim 28, wherein, when generation of the encryption key fails due to the service type, generating a Key Reject message including an error code indicating a failure reason and transmitting the generated Key Reject message to the subscriber station using a MAC message.

34. (New) The method as claimed in claim 33, wherein the base station sends an unsupported service type error code to the subscriber station when an encryption key for the service type corresponding to the an encryption key request of the subscriber station cannot be generated and distributed.

35. (New) The method as claimed in claim 33, wherein the base station sends an unauthorized multicast service group ID type error code to the subscriber station when the

service type for the encryption key requested by the subscriber station is a multicast service that is an unsupported multicast service for a specific multicast service group ID.

36. (New) An apparatus for requesting an encryption key in a wireless communication system, the apparatus comprising:

a transmitter for transmitting a first message requesting the encryption key to a base station;

a receiver for receiving a second message from the base station; and

a controller for determining a service type of a traffic connection, generating the first message including an identifier corresponding to the service type, transmitting the first message to the base station through the transmitter, and receiving the second message from the base station through the receiver.

37. (New) The apparatus as claimed in claim 36, wherein the first message is a key request message.

38. (New) The apparatus as claimed in claim 37, wherein the second message is a key reply message including the encryption key corresponding to the service type.

39. (New) The apparatus as claimed in claim 36, wherein the service type is one of a unicast service, a multicast service, and a broadcast service.

40. (New) The apparatus as claimed in claim 36, wherein when the service type is a multicast service, the first message includes an identifier of a multicast service group of a subscriber.

41. (New) The apparatus as claimed in claim 36, further comprising a memory for storing information including the traffic encryption key or an error code resulting from an analysis of an

message analyzer controlled by the controller.

42. (New) An apparatus for distributing an encryption key in a wireless communication system, the apparatus comprising:

a receiver for receiving a first message including an identifier corresponding to a service type of a traffic connection to request the encryption key from a subscriber station;

a generator for generating the encryption key corresponding to the service type;

a transmitter for transmitting a second message to the subscriber station; and

a controller for receiving the first message from the subscriber station through the receiver, generating the encryption key corresponding to the service type, and generating the second message including the encryption key.

43. (New) The apparatus as claimed in claim 42, wherein the first message is a key request message.

44. (New) The apparatus as claimed in claim 43, wherein the second message is a key reply message including the encryption key corresponding to the service type.

45. (New) The apparatus as claimed in claim 42, wherein the service type is one of a unicast service, a multicast service, and a broadcast service.

46. (New) The apparatus as claimed in claim 42, wherein when the service type is a multicast service, the first message includes an identifier of a multicast service group of a subscriber.

47. (New) The apparatus as claimed in claim 46, further comprising a Key Reject transmitter for transmitting a Key Reject message, which includes an error code, to the subscriber station using a MAC message when the controller generates an error for the request of the

encryption key from the subscriber station.